**AMENDMENTS TO THE CLAIMS**

Please amend the claims as follows:

1. (Original) A system for secure data transmission comprising: a session layer that maps authentication of at least one request to session level authorization, the authorization defining permitted communications between at least one resource and the at least one request.

2. (Original) The system of claim 1, wherein the session layer includes: a trusted session sub-layer for session level authorization and maintenance; and a reverse proxy for transferring data between the at least one resource and the at least one request.

3. (Original) The system of claim 2, wherein layers of the request below its trusted session sub-layer are unaware of existence of layers of the resource below its trusted session sub-layer.

4. (Original) The system of claim 1, wherein the session layer forms a bundle of transport layer connections between the at least one resource and the at least one request.

5. (Original) The system of claim 4, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

6. (Original) The system of claim 1, wherein the session layer maps ports onto itself.

7. (Original) The system of claim 6, wherein the session layer associates a transport connection for data to pass from the at least one resource to the at least one request.

8. (Original) The system of claim 1, further including a trusted operating system.

9. (Original) The system of claim 1, wherein the authorizations are dynamically updated.

10. (Original) The system of claim 1, wherein no layer below the session layer communicates on a peer to peer level.

11. (Original) The system of claim 1, wherein the session layer includes a sterile core.

12. (Original) The system of claim 1, wherein the session layer maps the authentication of users using a Secure Core rulebase.

13. (Original) The system of claim 1, wherein resource identities are masked.

14. (Original) The system of claim 1, wherein the authorization is dependent on a network interface of the at least one request.

15. (Original) The system of claim 1, wherein the session layer provides an audit trail.

16. (Original) The system of claim 1, wherein the session layer can establish multiple sessions with multiple requests, each session operating in a half-duplex manner.

17. (Original) The system of claim 1, wherein the session layer mediates resources between the at least one request and the at least one resource based on a credential set.

18. (Original) The system of claim 1, wherein the session layer mediates resources between the at least one request and the at least one resource based on a credential set, and wherein the session layer bundles transport layer communications between the at least one resource and the at least one request by associating the bundles with the credential set.

19. (Original) The system of claim 1, further including a multi-level operating system used as a proxy.

20. (Original) The system of claim 1, further including a Session Manager to communicate through higher OSI layers.

21. (Original) The system of claim 1, wherein no physical resource is time-division shared by the at least one resource requester and the at least one resource provider.

22. (Original) A system for secure data transmission comprising: a virtual air gap provided by: a trusted session sub-layer for session authorization and maintenance; a trusted operating system for session separation; and a reverse proxy for data transfer between a user and a resource provider.

23. (Original) The system of claim 22, wherein layers of the user below its trusted session sub-layer are unaware of existence of layers of the resource provider below its trusted session sub-layer.

24. (Original) The system of claim 22, wherein the trusted session sub-layer forms a bundle of transport layer connections between the user and the resource provider.

25. (Original) The system of claim 24, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

26. (Original) The system of claim 22, wherein a session layer, which includes the trusted session sub-layer, maps ports onto itself.

27. (Original) The system of claim 22, wherein the session authorization is dynamically updated.

28. (Original) The system of claim 22, wherein no layer below a session layer, which includes the trusted session sub-layer, communicates on a peer to peer level.

29. (Original) The system of claim 22, wherein the trusted session sub-layer maps user authentication using a Secure Core rulebase.

30. (Original) The system of claim 22, wherein the session authorization is dependent on network interface of the user.

31. (Original) The system of claim 22, wherein the trusted session sub-layer mediates resources between the user and the resource provider based on a credential set.

32. (Original) The system of claim 22, wherein the trusted session sub-layer mediates resources between the user and the resource provider based on a credential set, and wherein the trusted session sub-layer bundles transport layer communications between the user and the resource provider by associating the bundles with the credential set.

33. (Original) The system of claim 22, further including a multi-level operating system used as a proxy.

34. (Original) The system of claim 22, further including a Session Manager to communicate through higher OSI layers.

35. (Original) The system of claim 22, wherein no physical resource is time-division shared by the user and the resource provider.

36. (Original) A system for secure data transmission comprising: a trusted session sub-layer maintaining a virtual air gap between a plurality of resource requesters and a plurality of resource providers; a session manager for a transfer of data between the plurality of resource requesters and the plurality of resource providers.

37. (Original) The system of claim 36, wherein the trusted session sub-layer includes a reverse proxy for transferring data between the plurality of resource requesters and the plurality of resource providers.

38. (Original) The system of claim 36, wherein the trusted session sub-layer forms a bundle of transport layer connections between the plurality of resource requesters and the plurality of resource providers.

39. (Original) The system of claim 38, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

40. (Original) The system of claim 36, wherein the trusted session sub-layer maps ports onto itself.

41. (Original) The system of claim 40, wherein the trusted session sub-layer associates transport connections for data to pass from the plurality of resource requesters to the plurality of resource providers.

42. (Original) The system of claim 36, wherein authorizations for the plurality of resource requesters are dynamically updated.

43. (Original) The system of claim 36, wherein no layer below a session layer, which includes the trusted session sub-layer, communicates on a peer to peer level.

44. (Original) The system of claim 36, wherein the session layer mediates resources between the plurality of resource requesters and the plurality of resource providers based on each resource requester's credential set, and wherein the session layer bundles transport layer communications between the plurality of resource requesters and the plurality of resource providers by associating the bundles with the each resource requester's credential set.

45. (Original) The system of claim 36, wherein no physical resource is time-division shared by the plurality of resource requesters and the plurality of resource providers.

46. (Original) A system for secure data transmission comprising: a trusted session sub-layer for peer-to-peer communication between a plurality of resource requesters and a plurality of resource providers; a rulebase for authenticating authorization of the plurality of resource requesters on a dynamic basis, wherein the trusted session sub-layer forms a bundle of transport layer connections between the plurality of resource providers and the plurality of resource requesters.

47. (Original) The system of claim 46, wherein the trusted session sub-layer includes a reverse proxy for transferring data between the plurality of resource requesters and the plurality of resource providers.

48. (Original) The system of claim 46, wherein layers of each resource requester below its trusted session sub-layer are unaware of existence of layers of each resource provider below its trusted session sub-layer.

49. (Original) The system of claim 46, wherein the trusted session sub-layer maps ports onto itself.

50. (Original) The system of claim 46, wherein the authorizations for each resource requester are dynamically updated.

51. (Original) The system of claim 46, wherein no layer below the session layer communicates on a peer to peer level.

52. (Original) The system of claim 46, wherein the session layer mediates resources between the plurality of resource requesters and the plurality of resource providers based on each user's credential set, and wherein the session layer bundles transport layer communications between the plurality of resource requesters and the plurality of resource providers by associating the bundles with the each user's credential set.

53. (Original) A system for secure data transmission comprising: a session layer for a transfer of data between a plurality of resource requesters and a plurality of resource providers, wherein no peer-to-peer connections exist below the session layer; and a trusted session sub-layer maintaining a virtual air gap, wherein no physical resources are time-division shared between any resource provider and any resource requester.

54. (Original) A system for secure data transmission comprising: session layer means for mapping authentication of at least one request to session level authorization, the authorization defining permitted communications between at least one resource and the at least one request.

55. (Original) A system for secure data transmission comprising: virtual air gap means provided by: trusted session sub-layer means for session authorization and maintenance; a trusted

operating system for session separation; and reverse proxy means for data transfer between a user and a resource provider.

56. (Original) A system for secure data transmission comprising: trusted session sub-layer means maintaining a virtual air gap between a plurality of resource requesters and a plurality of resource providers; session manager means for transferring data between the plurality of resource requesters and the plurality of resource providers.

57. (Original) A system for secure data transmission comprising: trusted session sub-layer means for peer-to-peer communication between a plurality of resource requesters and a plurality of resource providers; a rulebase for authenticating authorization of the plurality of resource requesters on a dynamic basis, wherein the trusted session sub-layer means forms a bundle of transport layer connections between the plurality of resource providers and the plurality of resource requesters.

58. (Original) A system for secure data transmission comprising: session layer means for a transfer of data between a plurality of resource requesters and a plurality of resource providers, wherein no peer-to-peer connections exist below the session layer means; and trusted session sub-layer means maintaining a virtual air gap, wherein no physical resources are time-division shared between any resource provider and any resource requester.

59. (Original) A computer program product for secure data transmission comprising: a computer usable medium having computer readable program code means embodied in the computer usable medium for causing an application program to execute on a computer system, the computer readable program code means comprising: computer readable program session layer code means for mapping authentication of at least one request to session level authorization, the authorization defining permitted communications between at least one resource and the at least one request.

60. (Original) A computer program product for secure data transmission comprising: a computer usable medium having computer readable program code means embodied in the computer usable medium for causing an application program to execute on a computer system, the computer readable program code means comprising: computer readable program code means for a virtual air gap provided by: computer readable program code trusted session sub-layer means for session authorization and maintenance; a trusted operating system for

session separation; and computer readable program code reverse proxy means for data transfer between a user and a resource provider.

61. (Original) A computer program product for secure data transmission comprising: a computer usable medium having computer readable program code means embodied in the computer usable medium for causing an application program to execute on a computer system, the computer readable program code means comprising: computer readable program code trusted session sub-layer means for maintaining a virtual air gap between a plurality of resource requesters and a plurality of resource providers; computer readable program code session manager means for transferring data between the plurality of resource requesters and the plurality of resource providers.

62. (Original) A computer program product for secure data transmission comprising: a computer usable medium having computer readable program code means embodied in the computer usable medium for causing an application program to execute on a computer system, the computer readable program code means comprising: computer readable program code trusted session sub-layer means for peer-to-peer communication between a plurality of resource requesters and a plurality of resource providers; a rulebase for authenticating authorization of the plurality of resource requesters on a dynamic basis, wherein the trusted session sub-layer means forms a bundle of transport layer connections between the plurality of resource providers and the plurality of resource requesters.

63. (Original) A computer program product for secure data transmission comprising: a computer usable medium having computer readable program code means embodied in the computer usable medium for causing an application program to execute on a computer system, the computer readable program code means comprising: computer readable program code session layer means for transferring data between a plurality of resource requesters and a plurality of resource providers, wherein no peer-to-peer connections exist below the computer readable program code session layer means; and computer readable program code trusted session sub-layer means for maintaining a virtual air gap, wherein no physical resources are time-division shared between any resource provider and any resource requester.

64. (Original) A method for secure data transmission comprising: mapping authentication of at least one request to session level authorization in a session layer, the authorization defining permitted communications between at least one resource and the at least one request.